UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/924,391	08/07/2001	Tal Givoly	XACTP001	6261

28875 7590 06/29/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
TRAN, PHILIP B	
ART UNIT	PAPER NUMBER
2155	

DATE MAILED: 06/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

5

Office Action Summary	**Application No.** 09/924,391	**Applicant(s)** GIVOLY, TAL	
	Examiner Philip B. Tran	**Art Unit** 2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 February 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-5,7-11,13,14,16-20 and 23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-5,7-11,13,14,16-20 and 23* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This is in response to amendment filed on 17 February 2005. Claims 1, 11, 20 and 23 have been amended. Claims 2, 6, 12, 15, and 21-22 have been canceled. Therefore, claims 1, 3-5, 7-11, 13-14, 16-20 and 23 are pending for further examination.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3-5, 7-11, 13-14, 16-20 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Conklin et al (Hereafter, Conklin), U.S. Pat. No. 5,991,881 in view of Engel et al (Hereafter, Engel), U.S. Pat. No. 6,115,393.

Regarding claim 1, Conklin teaches a method for processing network accounting information, comprising receiving accounting information over a packet-switched network, monitoring at least one aspect of the received accounting information (= traffic information including attack data such as date/time, packet type, attack type source/destination addresses) [see Fig. 7], and after receiving the accounting information, discarding at least a portion of the accounting information based on the monitored aspect (i.e., network traffic measurement and monitoring for reporting information about captured packets and detecting intrusion into the network and into computers connected to the network for denial of service) [see Abstract and Figs. 6-9 and Col. 1, Line 10 - Col. 2, Line 4].

Conklin does not explicitly teach the portion of the accounting information is discarded to prevent an overload of subsequent processing. However, Engel, in the same field of network monitoring endeavor, discloses event manager (38) is managing the network and analyzing for statistical, accounting and alarm filtering and making decision on further action including discarding events and controlling in an overload situation [see Engel, Col. 12, Lines 7-67]. It would have been obvious to one of ordinary skill in the art at the time of the invention was made to incorporate the teaching of Engel into the teaching of Conklin in order to efficiently monitor and control the network account information for preventing the overload situation of information in the network.

Regarding claim 3, Conklin further teaches the accounting information is discarded for dealing with heavy network traffic (i.e., monitoring and analyzing the traffic communication) [see Fig. 6].

Regarding claim 4, Conklin further teaches generating a summary of the accounting information (i.e., reported of collected information and stored information in the database) [see Col. 4, Line 52 - Col. 5, Line 45].

Regarding claim 5, Conklin does not explicitly teach monitoring the at least one aspect of the received accounting information includes detecting a scan of a plurality of ports. However, Engel, in the same field of network monitoring endeavor, discloses event statistics including IP address and port numbers monitoring [see Engel, Col. 28, Lines 16-24]. It would have been obvious to one of ordinary skill in the art at the time of the invention was made to incorporate the teaching of Engel into the teaching of Conklin for scanning the ports in order to track down ongoing attacks and identifying potential intrusions on the network and system connected to the network.

Regarding claims 7-8, Conklin further teaches monitoring the at least one aspect of the received accounting information includes monitoring a rate of receipt of the accounting information and whether the rate of receipt of the accounting information exceeds a predetermined amount (i.e., monitoring and collecting network data such as traffic over time) [see Figs. 6-8 and Col. 4, Lines 30-67].

Regarding claim 9, Conklin does not explicitly teach monitoring the at least one aspect of the received accounting information includes monitoring a load on a system receiving the accounting information. However, Engel, in the same field of network monitoring endeavor, discloses monitoring and collecting statistic information such as traffic load [see Engel, Col. 10, Lines 57-67 and Col. 38, Lines 6-40]. It would have been obvious to one of ordinary skill in the art at the time of the invention was made to incorporate the teaching of Engel into the teaching of Conklin for monitoring a load on the system in order to avoid traffic congestion and overload problems.

Regarding claim 10, Conklin further teaches the network includes the Internet (i.e., using TCP/IP suggests the network attached to the Internet) [see Col. 3, Lines 15-21].

Claim 11 is rejected under the same rationale set forth above to claim 1.

Claims 13-14 are rejected under the same rationale set forth above to claims 3-4, respectively.

Claims 16-17 are rejected under the same rationale set forth above to claims 7-8, respectively.

Claim 18 is rejected under the same rationale set forth above to claim 5.

Claim 19 is rejected under the same rationale set forth above to claim 9.

Claim 20 is rejected under the same rationale set forth above to claim 1.

Regarding claim 23, Conklin teaches a method for processing network accounting information, comprising receiving accounting information over a packet-switched network, monitoring at least one aspect of the received accounting information (= traffic information including attack data such as date/time, packet type, attack type source/destination addresses) [see Fig. 7], and discarding at least a portion of the accounting information based on the monitored aspect (i.e., network traffic measurement and monitoring for reporting information about captured packets and detecting intrusion into the network and into computers connected to the network for denial of service) [see Abstract and Figs. 6-9 and Col. 1, Line 10 - Col. 2, Line 4].

Conklin further teaches generating a summary of the accounting information (i.e., reported of collected information and stored information in the database) [see Col. 4, Line 52 - Col. 5, Line 45], detecting a scan of a plurality of Internet Protocol (IP) addresses (i.e., detecting IP address) [see Col. 5, Lines 26-45 and Col. 6, Lines 44-60], and monitoring a rate of receipt of the accounting information and whether the rate of receipt of the accounting information exceeds a predetermined amount (i.e., monitoring and collecting network data such as traffic over time) [see Figs. 6-8 and Col. 4. Lines 30-67].

Conklin does not explicitly teach monitoring the at least one aspect of the received accounting information includes detecting a scan of a plurality of ports. However, Engel, in the same field of network monitoring endeavor, discloses event statistics including IP address and port numbers monitoring [see Engel, Col. 28, Lines 16-24]. It would have been obvious to one of ordinary skill in the art at the time of the invention was made to incorporate the teaching of Engel into the teaching of Conklin for scanning the ports in order to track down ongoing attacks and identifying potential intrusions on the network and system connected to the network.

In addition, Conklin does not explicitly teach monitoring the at least one aspect of the received accounting information includes monitoring a load on a system receiving the accounting information. However, Engel, in the same field of network monitoring endeavor, discloses monitoring and collecting statistic information such as traffic load [see Engel, Col. 10, Lines 57-67 and Col. 38, Lines 6-40]. It would have been obvious to one of ordinary skill in the art at the time of the invention was made to incorporate the teaching of Engel into the teaching of Conklin for monitoring a load on the system in order to avoid traffic congestion and overload problems.

4. Applicant's arguments with respect to claims 1, 3-5, 7-11, 13-14, 16-20 and 23 have been considered but are moot in view of the new ground(s) of rejection.

Other References Cited

5. The following references cited by the examiner but not relied upon are considered pertinent to applicant's disclosure.

A) Bullard, U.S. Pat. No. 6,625,657.

B) Schweitzer, U.S. Pat. Application Pub. No. US 2002/0038364 A1.

C) Bullard, U.S. Pat. No. 6,405,251.

6. A SHORTENED STATUTORY PERIOD FOR RESPONSE TO THIS ACTION IS SET TO EXPIRE THREE MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION. FAILURE TO RESPOND WITHIN THE PERIOD FOR RESPONSE WILL CAUSE THE APPLICATION TO BECOME ABANDONED (35 U.S.C. § 133). EXTENSIONS OF TIME MAY BE OBTAINED UNDER THE PROVISIONS OF 37 CAR 1.136(A).

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Philip Tran whose telephone number is (571) 272-3991. The Group fax phone number is (703) 872-9306. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar, can be reached on (571) 272-4006.

8. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Philip Tran
Philip B. Tran
Art Unit 2155
June 16, 2005